1985

# A Program Manager's handbook for system safety and Military Standard 882B

Duke, Boyce W.

Monterey, California. Naval Postgraduate School

# NAVAL POSTGRADUATE SCHOOL
## Monterey, California


# THESIS

A PROGRAM MANAGER'S HANDBOOK FOR
SYSTEM SAFETY AND MILITARY STANDARD 882B

Boyce W. Duke

March 1985

Thesis Advisor: Donald M. Layton

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

## REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

| | |
|---|---|
| 1. REPORT NUMBER | 2. GOVT ACCESSION NO. / 3. RECIPIENT'S CATALOG NUMBER |
| 4. TITLE *(and Subtitle)*: A Program Manager's Handbook for System Safety and Military Standard 882B | 5. TYPE OF REPORT & PERIOD COVERED: Master's Thesis March 1985 |
| | 6. PERFORMING ORG. REPORT NUMBER |
| 7. AUTHOR(s): Boyce W. Duke | 8. CONTRACT OR GRANT NUMBER(s) |
| 9. PERFORMING ORGANIZATION NAME AND ADDRESS: Naval Postgraduate School Monterey, California 93943 | 10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS |
| 11. CONTROLLING OFFICE NAME AND ADDRESS: Naval Postgraduate School Monteret, California 93943 | 12. REPORT DATE: March 1985 |
| | 13. NUMBER OF PAGES: 44 |
| 14. MONITORING AGENCY NAME & ADDRESS*(if different from Controlling Office)* | 15. SECURITY CLASS. *(of this report)*: UNCLASSIFIED |
| | 15a. DECLASSIFICATION/ DOWNGRADING SCHEDULE |

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for public release, distribution unlimited

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

System Safety, System Safety Engineering, Military Standard 882B

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

The Program Manager's role in the acquisition of new weapon systems encompasses many disciplines, some of which he may have little, if any, training or experience in handling. One of these areas, which until recent years has received little attention, is System Safety Engineering. This thesis is an attempt, in handbook form, to introduce the Program Manager to

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

S/N 0102-LF-014-6601

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

the System Safety Process and provide basic guidance in the application of MIL STD 882B, the governing Department of Defense directive on system safety program requirements.

Approved for public release; distribution is unlimited.

# A Program Managers Handbook for System Safety and Military Standard 882B

by

Boyce W. Duke
Lieutenant Commander, United States Navy
B.A., University of California, Santa Barbara, 1969

Submitted in partial fullment of the
requirements for the degree of

MASTER OF SCIENCE IN AERONAUTICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
March 1985

# ABSTRACT

The Program Manager's role in the acquisition of new weapon systems encompasses many disciplines, some of which he may have little, if any, training or experience in handling. One of these areas, which until recent years has received little attention, is System Safety Engineering. This thesis is an attempt, in handbook form, to introduce the Program Manager to the System Safety Process and provide basic guidance in the application of MIL STD 882B, the governing Department of Defense directive on system safety program requirements.

# TABLE OF CONTENTS

## ACKNOWLEDGEMENT

I would like to acknowledge the invaluable assistance of Professor Donald M. Layton in this endeavor. His knowledge of System Safety, his encouragement, and his overall support made this a most interesting and rewarding experience.

# I. INTRODUCTION

Safety has always been a consideration in the systems acquisition/procurement and design process, however its primary emphasis has been centered on the operational phase of the system's life cycle. With the ever increasing cost of retrofiting or replacing operational weapon systems, it became evident that safety had to enter the design and procurement process at the earliest point possible and be an active consideration throughout the system's life cycle. To accomplish this increased safety consciousness, System Safety Engineering, or simply System Safety, was brought into the process.

System Safety is defined in Military Standard 882B [Ref. 1] as "the application of engineering and management principles, criteria, and techniques to optimize safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle." The primary function of System Safety is the early identification and classification of hazards so that action may be taken to correct the hazards prior to reaching final design decisions. The earlier an unacceptable hazard is identified and eliminated, the less the negative impact on a project and the less the likelihood of a costly retrofit.

The person having the ultimate responsibility for the implementation of a system safety program for new acquisistions is the Program Manager. Though most Program

Managers have been carefully screened and have had training in acquisition management, one area of unfamiliarity and weakness is often that of implementing MIL STD 882B and maintaining an effective system safety effort.

It is the objective of this thesis to assist the Program Manager in his duties involving system safety management by providing a usable handbook to introduce him to the principles of system safety and then to provide practical guidance for the implimentation of MIL STD 882B.

## II. BACKGROUND

Prior to the adoption of System Safety as a formal discipline, safety was an ad hoc methodology, with little effort being made to actually design safety into the systems. Once operational, a "fly-it, fix-it, fly-it" approach was taken. Hazards which were identified during operational use were either judged to be of low risk or fixed by retrofit. In either case, weight and/or cost penalties were considered acceptable. Due to the relative inexpensiveness of the systems and the abundance of raw materials, it simply was not cost effective to make System Safety a major design factor.

Due to the ever increasing complexity of new systems and skyrocketing cost of production which accompanied modern technology, System Safety gradually evolved into what it is today. It was no longer feasible to wait for hazards to appear in the operational phase since system replacement and retrofit costs had grown astronomically. It became apparent that if safety was designed into systems, life cycle cost could be reduced and system reliablity increased. With this realization came a multitude of instructions and directives from every direction and it was soon evident that a standardized approach to system safety was required for all the services. To this end, MIL STD 882 and its subsequent revisions were written.

MIL STD 882B, currently in effect, provides "uniform requirements for developing and implementing a system safety program of sufficient comprehensiveness to identify the hazards to a system and to impose design requirements and management controls to prevent mishaps by eliminating hazards or reducing associated risk to a level acceptable to the managing activity (MA)." [Ref. 1] This standard provides specific system safety tasks for both management and engineering which may be imposed on all applicable DOD acquisitions. The key individual in this process is the Program Manager, for it is he who serves as the MA and decides which tasks are appropriate for the program under his control. This selection or tailoring of tasks to fit the program is the first, the most difficult, and the most important step in the implementation of MIL STD 882B. Once accomplished, the Program Manager's primary system safety functions are to monitor and assist the efforts of the contractor in adhering to the establish System Safety Plan.

## III. METHODOLOGY

The basic premise in preparing this handbook was to keep it simple and usable, not just another huge volume filled with fact after fact that is read once, if that, and then due to its appalling nature, stuck away and never seen again. This handbook was to be a basic reference which could be keep at the program managers desk and repeatedly used to in his system safety endeavors. Accordingly, a limit of 30 pages was established. Within these pages, there was to be sufficient material to provide a sound introduction to the concepts of System Safety and to provide practical guidance for the implementation of MIL STD 882B.

The handbook first endeavors to impart an insight into the importance of System Safety in the procurement process and then present the general principles and fundamentals of system safety. Once this is accomplished, practical guidance and logical considerations in the implementation of MIL STD 882B are presented. Here specific elements of the standard are highlighted and then the standard is applied to three distinct weapon system acquisitions to obtain a baseline selection of system safety tasks. To aid in the selection process, a "Task Element Applicability Checklist" is provided. With the aid of this checklist, program managers can accurately make a baseline selection of tasks to include in the system safety program for their

project. It must be understood that this is only a "baseline selection" and that it must be molded to the project at hand after careful consideration of all available information.

Ideally, with the aid of this simple manual, program managers should have a clearer understanding of the system safety process and how to effectively apply MIL STD 882B to the management of any project under their cognizance. It should be noted that even though discussions are limited to weapon system acquisitions, the same fundamental principles apply to facilities acquisitions.

# IV. CONCLUSIONS

System Safety is an essential element in the acquisition of the weapon systems required for the defense of our nation. It is therefore paramount that anyone in position to exercise control over the implementation of MIL STD 882B (usually the Program Manager) fully understand the importance of system safety to the acquistion process.

This handbook is an initial attempt to aid the program manager in the management of the system safety aspects of the program. It is not designed to be a definitive reference to answer every relevant question on the subject. Hopefully, however, it should better equip the Program Manager to accurately estimate the complexity of the system safety effort and to effectively apply MIL STD 882B to the management of any given project.

To ensure that the above has been accomplished without any serious omissions or errors, it is strongly recommended that the handbook be reviewed by appropriate agencies prior to full distribution.

APPENDIX A

## A PROGRAM MANAGERS INTRODUCTION TO SYSTEM SAFETY AND MILITARY STANDARD 882B

### A. INTRODUCTION

This manual is not designed to answer every question on the topic of System Safety Engineering. It endeavors, however, to impart an insight into System Safety and the importance it plays in the procurement process. Additionally, practical guidance and logical considerations for the application of Military Standard 882B to weapon system procuements is provided. To achieve this end, first the general principles and fundamentals of system safety engineering are presented. Secondly, specific areas of MIL STD 882B are highlighted, and lastly, to assist in the actual implementation of MIL STD 882B, it is applied to three separate weapon system procurements:

(1) Procurement of a major weapon system (a new aircraft).

(2) Procurement of a minor weapon system (a remotely piloted aircraft).

(3) Procurement of a modification/addendum to a weapon system (an radar upgrade for an in-service aircraft).

The above projects vary greatly in their scope and complexity and each requires a system safety effort tailored specifically to meet its individual needs. With the aid of this manual, one should have a clearer understanding of the system safety process and be better

equipped to accurately estimate the complexity of the system safety effort related to a given project and then be able effectively apply MIL STD 882B to the management of that project.

## B. SYSTEM SAFETY -- WHAT IS IT?

MIL STD 882B defines System Safety as "the application of engineering and management principles, criteria, and techniques to optimize safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle." Notice specifically the references to "optimize" and to "constraints". System Safety is not to be feared as an all consuming monster, blind to the limitations of one's particular project. It must be considered as one of the elements to be optimized along with many others. Also take note that it applies to "all phases of the system life cycle". While safety has always been a consideration in any new procurement or design process, its primary emphasis has always been affixed to the operational phase of the life cycle. Now, however, it extends throughout the design, operation, and disposal of the system.

## C. THE FUNCTION OF SYSTEM SAFETY

The primary function of System Safety is the early identification and classification of hazards in order that

measures may be taken to eliminate the hazards prior to reaching final design decisions. The earlier an unacceptable hazard is identified and eliminated or controlled, the less the negative impact on the project and the less the likelihood of a costly retrofit.

## D. DEVELOPMENT OF SYSTEM SAFETY

In the past, when systems were relatively inexpensive and raw materials were plentiful, System Safety was an ad hoc methodology. Little effort was made to design safety into systems except to eliminate obvious hazards or those hazards known to exist from previous experience. Once operational, the "fly it - fix it - fly it" method was utilized. Any identified hazard was eliminated through retrofit or judged to be low risk items not requiring retrofit. In either case, the weight and/or cost penalty was considered acceptable. It simply wasn't cost effective to make System Safety a major design consideration.

As system complexity grew, the role of System Safety gradually changed to what it is today. Systems were no longer inexpensive or easy to manufacture, the design process became more sensitive to changes, and size/weight tolerances became more critical. It was no longer feasible to wait for hazards to appear in the operational phase because system replacement and retrofit costs had grown astronomically. It soon became evident that designing safety

into a system could reduce life cycle costs and increase the system's reliability. "Fly it - fix it - fly it" became "identify - analyze - eliminate".

Initial efforts to emphasize System Safety resulted in various instructions and directives being issued by each of the services. It soon, however, became apparent that a standardized approach applicable to all the services and all varieties of procurement was required. To this end, MIL STD 882 and its subsequent revisions were written. This standard made the developement of a System Safety program a requirement and defined the roles of the Program Manager and the contractor in implementing the program.

## E. SYSTEM SAFETY PROGRAM PLANNING AND COSTS

A System Safety Program is a formal program with definitive steps to ensure that safety is designed into systems, subsystems, and support equipment. It is to be set forth in the Statement of Work (SOW) of the Request for Proposal (RFP) and in the Contract Data Requirements List (CDRL). In general, it specifies procedures, standards, and testing requirements for the stated purpose of identifying and eliminating or controlling safety hazards. In that it is a part of the SOW and requires the expenditure of manpower and material assets, its cost must be included in that project budget. This is where far too many safety efforts meet their untimely demise--at the budget chopping

block. While the dollars expended on a safety effort is a quantifiable figure, the benefits reaped from the effort are not. Estimates of systems and lives saved by a safety program are just that--estimates for which no tangible dollar savings can be shown. While the cost effectiveness is difficult to show and impossible to prove, it is the Program Manager's job to ensure that System Safety is given careful attention and adequate funding.

## F. THE SYSTEM SAFETY PROCESS

The System Safety Process is simply the logical application of the System Engineering approach to obtain the desired System Safety objectives. The primary elements of this process are as follows:

(1) Lessons Learned - Probably the greatest proof for the necessity of a strong System Safety program are the multitude of accident and mishap reports. Analysis of these reports have shown that a great percentage of incidents are the result of a design flaw that could have been eliminated if safety had been given its just place in the design process. Use these reports to prevent the same design flaws in new projects and whenever practical, utilize systems and subsystems with proven track records.

(2) System Specifications - Precise definition of the system and its bounds, being careful to include all required maintenance and support facilities and/or equipment and the anticipated operating environments.

(3) System Hazard Analysis - This is an evaluation of the complete system to uncover any design features, system components, or any system interfaces that might lead to or create a hazard. Fault tree analysis (FTA) and failure mode and effects analysis (FMEA) are often used for this purpose.

(4) Hazard Identification, Categorization, and Evaluation - The hazard analysis will lead to the identification of system hazards, which must then be categorized as to potential danger and the probability of their occurrence. Using this information, careful evaluation must take place to determine which hazards require design changes due to either their severity or frequency of occurrence or a combination of the two.

(5) Action to Eliminate or Control Hazards - The old cliche "actions speak louder than words" applies here. All the analysis and evaluation serves no purpose if the appropriate corrective action is not taken. Measures must be taken to track every hazard until it is closed-out as directed.

(6) Modification of System Elements - The above steps are iterative in nature. Once a modification is made, a re-evaluation must be done to see if the hazards were corrected or if any new hazards were introduced.

(7) Effectiveness Evaluation - Included in this area are Mishap Analysis and System Test and Demonstration. This is done to verify the mission and cost effectiveness of the modifications. The question that must be answered is "Does the system still meet design specifications with the incorporated changes and have these changes eliminated or controlled the known hazards?"

(8) Increased Safety Assurance and Re-application - The resulting system is safer while still meeting the mission requirements and the lessons learned are utilized for future systems.

## G. SYSTEM SAFETY DEFINITIONS

The following definitions in conjunction with those provided in para 3.1 of MIL STD 882B are terms with which one must be familiar when working in System Safety:

(1) Contributing hazard - A condition which aides in the fulfillment of a hazardous event.

(2) Failure Mode and Effects Analysis (FMEA) - A qualitative technique which evaluates the effects of various failure modes on the safety of the system.

(3) Fault Hazard Analysis (FHA) - Similar to an FMEA, but includes consideration of human error, procedural deficiencies, environmental conditions and other events that might cause "normal" operations at an undesired time and result in a hazardous condition.

(4) Fault Tree Analysis (FTA) - A top-down evaluation technique which begins with an undesired event and proceeds through the system to identify the event or combination of events which would have to occur to cause the undesired event.

(5) Hazard Action Report (HAR) - A report which identifies an existing hazard, the probability and criteria for its elimination or control, a history of action taken and verification that the criteria has been met.

(6) Initiating hazard - A hazard or event which triggers a sequence of hazardous events.

(7) Primary hazard - A hazard which directly and immediately causes injury, death, damage, loss of equipment, degradation of capabilities, or loss of material.

(8) Sneak Circuit Analysis - A computer aided process for examinination of software and hardware to identify latent (sneak) circuits and conditions which inhibit desired functions or cause undesired functions without a component failure.

## H. MILITARY STANDARD 882B

Military Standard 882B provides "uniform requirements for developing and implementing a system safety program of sufficient comprehensiveness to identify the hazards to a system and to impose design requirements and management controls to prevent mishaps by eliminating hazards or reducing associated risk to a level acceptable to the managing activity (MA)". While MIL STD 882B, in many respects, is very similar to its predecessor, it goes

beyond and provides task elements for both management and engineering/design. These tasks are to be tailored by the MA to establish a safety program which meets the specific needs of each procurement. Herein lies the heart of the MA's role in the system safety effort--to evaluate each project and select the appropriate tasks for incorporation to contractual document. Once this is accomplished, the MA's must monitor and assist the efforts of the contractor in adhering to the established System Safety Plan.

## I. SYSTEM SAFETY REQUIREMENTS AND PRECEDENCE

In order to properly evaluate projects and accurately select appropriate tasks elements, the MA must first understand the basic requirements and precedence laid down by the military standard. To this end a brief summary of the major elements is provided below:

(1) The contractor shall establish and maintain an effective and efficient system safety program. A statement to this effect must be included in the SOW and CDRL.

(2) Safety, consistent with mission requirements, is to be designed into the system in a cost effective manner. Hazards are to be identified, evaluated and eliminated or reduced to a level acceptable to the MA.

(3) Prior to system design, all applicable standards, specifications, regulations, historical data and lessons learned shall be reviewed for guidance. During the project, thorough documentation of all hazards shall be maintained and significant safety data should be documented and submitted as lessons learned.

(4) The precedence for the handling of identified hazards begins with the elimination or reduction to a level acceptable to the MA through design changes. If this is not possible, appropriate safety devices are to be incorporated. Next in precedence is the incorporation of hazard detection and warning devices to warn personnel of the hazard. If all the above are impractical, procedures and training shall be used to reduce the risk. However, "without specific waiver, no warning, caution, or other written advisory shall be used as the only risk reduction method for a Category I or II hazard...."

J. RISK ASSESSMENT

Effective implementation of a system safety program requires proper assessment of the risk associated with any identified hazard. Once this has been accomplished, hazards may be prioritized in order that the potential risk and the costs to reduce that risk may we properly weighed and design decision made. To perform this prioritization, it is necessary to consider both hazard severity and hazard probability.

Hazard severity primarily concerns the magnitude or criticality (category I is catastrophic, II is critical, etc.) to personnel safety or the successful mission accomplishment and is qualitative in nature. Hazard probability, however, is a measure of the likelihood of occurrence of an event and though usually associated with a quantifiable number, is often categorized qualitatively (frequent, occassional, etc.). Though prioritization may be simply a subjective evaluation of the above, it is usually advantageous to utilize a risk assessment matrix

(Figures 1 and 2 of Appendix A to MIL STD 882B provide two samples of matrices) to provide qualitative prioritization factors.

One note of caution when performing risk assessment on projects that were contracted when MIL STD 882 was effective. Under 882, the hazard severity description and category numbers where reversed (catastrophic was category IV). Contracts under 882A agree with 882B.

## K. MIL STD 882B AND THE LIFE CYCLE PROCESS

As stated previously, the system safety effort is to extend through all phases of the life cycle process, and it is important to be familiar with the safety requirements of each of these phases. Accordingly, a summary of the primary system safety aspects of each phase is provided.

## L. CONCEPTUAL/DEVELOPMENT PHASE

In this phase, the system safety activities are divided into two primary functions--one for the system and one for the program. For the system, a determination of the state of safety and the requirements for safety for the various alternatives under consideration must be made. It is this determination that will ultimately provide the grounds for design decisions. Key elements in this area are a thorough delineation of the operational and support requirements of the system, a review of applicable "Lessons Learned", the

performance of a Preliminary Hazard Analysis (PHA) and associated review/design decision processes and documentation.

The safety activities for the program involve getting the system safety effort rolling in such a manner that it will continue throughout the life cycle. The earlier the program is put into effect, the more effective it will be. The primary item here is the development of the System Safety Program Plan (SSPP). The SSPP is normally written by the contractor but for smaller programs it may be written by the MA to reduce expenses. While the SSPP should address the entire life cycle, its primary emphasis may be focused on this phase since a review and update of the SSPP is essential to each phase. It is also essential that the System Safety Working Group be established and take an active part in the review of design proposals and of the PHA.

## M. DEMONSTRATION/VALIDATION PHASE

The safety objectives of this phase are, as the name indicates, to demonstrate and validate that the designs of the conceptual phase meet the desired specifications while maintaining a satisfactory level of system safety. The first step in accomplishing this goal is the review/update of the SSPP by the MA. This is done to ensure that an integrated system safety effort is provided, since it is in

this phase that the system safety effort is the most intensive.

Much of the system safety effort will involve conducting numerous hazards analyses, such as the System Hazard Analysis (SHA), the Subsystem Hazard Analysis (SSHA), etc. Each of these analyses is designed to verify that system safety is achieved in a particular area of interest. Once these analyses have been completed, measures must be taken to ensure that the hazards are properly rectified. This is accomplished by the implimentation of a hazard tracking scheme which follows a hazard from discovery and documentation to ultimate reconciliation.

Test and evaluation procedures are to be reviewed from a system safety aspect to ensure that no hazards are introduced by test procedures. Additionally, training plans, logistics and support plans, etc, must be reviewed for safety considerations, and an advance look at the projected production process and operations should be conducted.

Finally, and most importantly, it must be verified that what has been learned in this phase is added to the requirements documents (SOW, Specs, etc) to ensure inclusion in the following phases. The bottom line is to ensure that system safety objectives are achieved while still meeting design requirements and specifications and

keeping within cost restraints. This is easy to say, but more often than not, very difficult to accomplish.

## N. FULL SCALE DEVELOPEMENT

Here the transformation of validated designs into full scale production occurs. This is followed by rigorous testing and analysis to ensure that the design lives up to expectations. System safety's role, for the most part, is a continuation of efforts started in the previous phase.

First the SSPP is reviewed and updated. If multiple subcontractors are involved, an Integrated System Safety Program Plan (ISSPP) is usually advisable. The ISSPP is designed to coordinate the system safety efforts of the subcontractors with those of the primary contractor. Engineering designs must be reviewed to ensure incorporation of safety requirements and that hazards previously identified have been corrected. All the various hazard analyses may require updating in as much as here will be the first chance to analyze the actual hardware and software items and to see actual full system interface.

All tests conducted during this phase must be reviewed to ensure that no further hazards have developed and that the system is indeed ready for production. Additionally, a look ahead at the production facilities should be made to verify that they are ready to safely handle the forthcoming tasks. Finally, the system safety effort in this phase

must be documented and the program should be tailored for the production/deployment phase.

## O. PRODUCTION AND DEPLOYMENT PHASE

The primary system safety objective of this phase is to ensure that the system is produced in accordance with the approved specifications and designs and that, after post-production tests, it is deployed to the fleet for operational use. To accomplish this task, first the SSPP is updated to reflect the requirements of the phase. Safety controls and inspections of the production process and operations must be enforced. Evaluation of testing of early production hardware/systems must be performed to detect and correct any additional safety hazards. Various Engineering Change Proposals (ECP) and Notices of Exception (NOE) will most likely be submitted and must be reviewed for their impact on system safety.

Once the system is actually deployed, fleet use invariably defines new, unexpected hazardous modes of operation and new procedures. NOE's and ECP's associated with these findings must again be evaluated for safety impact and acted on accordingly.

## P. DISPOSAL PHASE

Though disposal of newly developed systems is not usually an immediate worry, the system safety effort is not

complete until this phase is considered. The SSPP should contain provisions for the safe disposal of the system and any of its components which might present potential hazards. Items to consider are health hazards, contamination, recyclability, etc.

Q. SELECTION OF TASK ELEMENTS

As previously stated, the heart of the system safety effort for the MA is the selection of the task elements which will meet the program safety requirements in a cost effective manner. Once selected, these tasks are then included in the SOW and will specify the contractual system safety requirements for the program. In order to properly select the appropriate tasks for a given project, the MA must have a clear understanding of the system requirements, specifications, program phases, and the safety requirements identified by higher authorities. Once this is well in hand, tailoring of MIL STD 882 system safety tasks may commence.

To aid in the task selection/tailoring process, MIL STD 882B has provided Tables 1 and 2 and Section 50 to Appendix A for general guidance. The material presented therein, is summarized and/or expanded in the following "Task Element Applicability Checklist" (TEACL) in a manner designed for clarity and quick reference. After a brief description of a task, the TEACL will specify the usual program/life cycle

phases of applicability and then present specific points to assist in determining if the task is required/desired. Utilization of this checklist format will enable the MA to determine a baseline selection of system safety task requirements which can then be weighed against project requirements and cost constraints. Remember, however, that a hasty elimination of task elements might well result in future design flaws and ultimately greater expenditures of both time and money.

R. TASK ELEMENT APPLICABILITY CHECKLIST

TASK 100 (System Safety Program) - Requires the contractor to implement a system safety program.

.... - REQUIRED whenever MIL STD 882B is imposed.

TASK 101 (System Safety Program Plan) - Requires that a SSPP be developed which will serve as the basis of understanding between the contractor and MA on how the system safety requirements will be achieved.

.... - Applicable to all phases.

.... - Highly recommended for all MIL STD 882B procurements.

TASK 102 (Integration/Management of Associate Contractors, Subcontractors, Architect and Engineering

Firms) - Provides the primary contractor and MA with a means of establishing and maintaining an integrated system safety effort with other contractors on a project. The ISSPP is the basis of this integration.

.... - Applicable to all phases.

.... - Generally needed only on major systems where numerous contractors are involved.

TASK 103 (System Safety Program Reviews) - This task requires the contractor to periodically report on the status of the system safety program to the MA. This is in addition to safety activities at milestone design reviews.

.... - Applicable to all phases.

.... - Recommended for early phases of most projects. (Frequency of reviews vary with project and/or system complexity.)

.... - May be needed to meet requirements for munition safety boards, first flight readiness reviews, etc.

TASK 104 (System Safety Group/System Safety Working Group) - The group assists the MA in the management of the system safety program.

.... - Applicable to all phases.

.... - Generally required by service regulations for all major projects.

TASK 105 (Hazard Tracking and Risk Resolution) - A procedural method to document and follow all identified hazards until ultimate resolution.

.... - Applicable to all phases.

.... - Critical to most projects to ensure proper disposition of all hazards.

TASK 106 (Test and Evaluation Safety) - The purpose of this task is to ensure that additional specific attention is given safety in the test and evaluation process.

.... - Applicable primarily to the Conceptual and Demonstration/Validation Phases.

.... - Recommended for all major weapon systems and for minor systems where hazards to life are evident.

TASK 107 (System Safety Progress Summary) - This task requires the preparation of periodic reports on the status of the system safety effort.

.... - Applicable to all phases.

.... - Recommended for major projects and a good option for all projects if funding permits.

TASK 108 (Qualification of Key Contractor System Safety Engineers/Managers.) - Establishs qualifications for contractor system safety personnel.

.... - Applicable to all phases.

.... - Generally selected only for major projects but usually not necessary since contractors will normally select well qualified personnel to protect their own interests.

TASK 201 (Preliminary Hazard List) - Requires the compilation of a preliminary list of potential hazards which will enable the MA to better direct emphasis in the system safety program.

.... - Applicable only to the early Conceptual Phase.

.... - Recommended for any project to get an early indication of inherent safety design flaws.

TASK 202 (Preliminary Hazard Analysis) - Requires performing and documenting a PHA to establish an initial risk assessment of the concept or system. It will examine alternate methods to reduce safety hazards while still meeting specifications/requirements.

.... - Primarily applicable to earlier phases.

.... - Recommended for all projects.

TASK 203 (Subsystem Hazard Analysis) - Requires in depth analysis of safety hazards associated with the design of each subsystem.

.... - Primarily applicable to Demonstration/Validation and Full Scale Development Phases.

.... - Recommended for projects where multiple major subsystems are involved.

TASK 204 (System Hazard Analysis) - Requires performance of a SHA which examines the interface of all subsystems in the operation of the system and how the failure modes affect the overall safety of the system.

.... - Primarily applicable to Demonstration/Validation and Full Scale Development Phases and to lesser extent design changes in the Production and Deployment Phase.

.... - Recommended for projects of all levels, since even for a modification/addendum, a thorough SHA is advisable to ensure no safety hazards have been introduced.

TASK 205 (Operating and Support Hazard Assessment) - This task requires analysis of hazards associated with the environment, personnel, procedures and equipment.

.... - Applicable to all but Conceptual Phase.

.... - Recommended for all major or minor projects with significant personnel interface/support require ments or extreme environmental conditions.

TASK 206 (Occupational Health Assessment) - This task performance documents health hazards associated with a

system and recommends protective measures to reduce the risk to an acceptable level.

.... - Applicable to all phases.

.... - Recommended when toxic materials or physical agents (cold, heat, noise, radiation, etc) are involved.

TASK 207 (Safety Verification) - Requires that test/demonstrations be performed to verify compliance with safety requirements for safety critical items.

.... - Applicable to Demonstration/Validation and and Full Scale Development Phases.

.... - Required when system specification/requirements and/or regulations/standards state that specific safety guidelines be met.

TASK 208 (Training) - Requires certification and training of personnel involved in the development, test, and operation of the system.

.... - Applicable to all but Conceptual Phase.

.... - Generally not needed when dealing with established governmental contractors.

TASK 209 (Safety Assessment) - This task requires the contractor to document any residual safety problems and special controls/procedures associated with the system.

.... - Generally applicable to any phase.

.... - Recommended for most projects. (If funding constraints require, this can be eliminated for minor projects. Though the information provided is generally available elsewhere, this can be a single source of critical safety information.)

TASK 210 (Safety Compliance Assessment) - Requires documentation of compliance with contractually imposed regulation, standards and laws to ensure safe system design.

.... - Generally applicable to all phases.

.... - Recommended for all major programs and required for any program where regulations apply.

.... - For low safety risk minor programs and/or modification/addendums, it may be the only safety analysis.

TASK 211 (Safety Review of ECP's and Request for Deviation/Waivers) - Requires documented analysis of ECP's and Requests for Deviation/Waiver.

.... - Applicable to all but Conceptual Phase.

.... - Recommended for all major/minor weapon system procurements.

TASK 212 (Software Hazard Analysis) - Requires analysis of software to ensure that safety hazards are not inadvertantly introduced by software interaction.

.... - Applicable to all but Conceptual Phase.

.... - Recommended for any procurement in which critical systems/subsystems are software controlled.

TASK 213 (GFE/GFP System Safety Analysis) - Requires that GFE/GFP items are considered in a safety analysis.

.... - Applicable to all but Conceptual Phase.

.... - Recommended only when GFE/GFP items interface directly with new contractor developed hardware or software in a new system.

## S. APPLICATIONS OF MIL STD 882B

In the following three sections, the MIL STD 882B is applied to three distinct weapon system acquisitions in order to demonstrate its application at various levels of system complexity and fiscal expenditure. In each case, the nature of the acquisition is described and then some of the considerations in the application of the military standard are weighed. Next, though not discussed in detail, the TEACL has been utilized to make a baseline selection of MIL STD 882B task elements for inclusion into a comprehensive system safety program. The results of this baseline selection are summarized in Table I. It is important to remember that this is only a baseline selection to put the MA over the first hurdle. After this selection is made, the MA must painstakingly weigh the

myriad of factors/constraints affecting each individual project to develop a system safety program that is suited to the project at hand.

## T. MAJOR WEAPON SYSTEM APPLICATION

Here MIL STD 882B is applied to the acquisition of a replacement for the F/A-18 Hornet, an all weather fighter and attack aircraft. Examining the operating environment and aircraft missions several items are evident which will aid in task selection. Its primary operational environment will be off a carrier with all the associated hazards. It will have guns and carry an assortment of air-to-air and air-to-surface weapons. Its radar and avionics suite will be highly software dependent, as most likely will be the flight control system. It will be a massive project with numerous sub/associate contractors. As Table I shows, any acquisition of this magnitude mandates an extensive system safety effort. Failure to identify and correct safety hazards during development may result in loss of lives and valuable aircraft, high retrofit expenditures and possibly affect national security. Items selected here for a baseline should, except under extreme funding limitations, make up the final task selection package.

## U. MINOR WEAPON SYSTEM APPLICATION

Here the military standard is applied to the acquisition of 100 remotely piloted vehicle/aircraft (RPV). They will be used for battlefield surveillance by the Marines and will be launched and recovered at remote airstrips. Additionally, it is anticipated that hot-refueling will often be required to support ground operations. It will be assumed that the decision has been made to cut cost by purchasing a commercially available aircraft and add surveillance, communications, and control equipment. Additionally, much of the equipment to be installed will be off-the-shelf/GFE items. The greatest chance of hazards to life will be from loss of RPV control and from hot-refueling accidents. Since the aircraft and much of the necessary equipment will already be proven, it will be necessary to develop the control system and software, test them separately and then test the integrated system.

While the above program is far less complex than the previous one, the system safety effort, though reduced, is still substantial. As shown in Table I, with the exception of the SSHA, most of the same engineering analyses and task should still be conducted. The greatest change is in the management tasks where significant reduction has occured.

V. MODIFICATION/ADDENDUM APPLICATION

Here MIL STD 882B is applied to the development and retrofit of an advanced radar system for an in-service aircraft. The upgrade has been required to keep pace with a newly developed air-to-air missile who's range surpasses that of the aircraft's current radar. It is clearly evident that an effective system safety effort can be accomplished with relatively minimal task imposition since there is little chance that this change could induce significant safety hazards. The tasks selected are shown in Table I. It is important to note that even though only a few tasks have been selected, management has been directed to incorporate system safety into the system's development (Tasks 100 and 101) and that engineering is required to conduct sufficient analyses to determine that no new safety hazards have been introduced into the current aircraft due to this update.

W. NOW OR LATER

This manual has presented basic information and provided guidance on the application of System Safety Engineering and MIL STD 882B to the military weapon system acquisition process. Utilizing the information herein, one should be better able to effectively apply MIL STD 882B to any given program. Again, it is important to realize that no two programs are alike and that the baseline task

selection obtained with the TEACL is just that--a baseline which must be molded to the individual program.

Every program manager has the responsibiltiy of implementing a system safety program for systems under his cognizance and MIL STD 882B provides an effective method for doing just that. Although short term costs are incurred, life cycle costs are reduced because of fewer accidents, lower maintenance down time, and fewer retrofit requirements and most importantly, lives will be saved. The extent to which these savings are realized is directly dependent on the program manager's commitment to the system safety program. Taking a phrase from an old TV commercial, "you can pay me now, or you can pay me later". The prudent program manager will do the former.

Table 1. MIL STD 882B Application Matrix

| TASK NUMBER | AIRCRAFT | RPV | RADAR |
|---|---|---|---|
| 100 | REQD | REQD | REQD |
| 101 | R | R | R |
| 102 | R | N | N |
| 103 | R | F | N |
| 104 | R | N | N |
| 105 | R | R | N |
| 106 | R | R | O |
| 107 | R | O | N |
| 108 | O | O | N |
| 201 | R | R | R |
| 202 | R | R | R |
| 203 | R | O | N |
| 204 | R | R | O |
| 205 | R | R | N |
| 206 | O | O | O |
| 207 | O | O | N |
| 208 | F | F | N |
| 209 | R | R | R |
| 210 | R | R | R |
| 211 | R | R | N |
| 212 | R | R | N |
| 213 | O | R | N |

R - recommended
O - optional/or if TEACL conditions met
F - include if funding permits
N - not necessary

# LIST OF REFERENCES

1. Department of Defense, System Safety Program Requirements, MIL STD 882B, 30 March 1984.

# BIBLIOGRAPHY

Hammer, W., Occupational Safety Management and Engineering, Prentice-Hall, 1981

Layton, D. M., System Safety Engineering Class Outline and Notes, Naval Postgraduate School, June 1984.

Naval Safety Center, System Safety for Program Managers, April 1982.

Rodgers, W. P., Introduction to System Safety Engineering, Wiley, 1971.

Roland, H. E. and Moriarty, B., System Safety Engineering and Management, Wiley, 1983.

# INITIAL DISTRIBUTION LIST

| | | No. Copies |
|---|---|---|
| 1. | Defense Technical Information Center<br>Cameron Station<br>Alexandria, VA 22314 | 2 |
| 2. | Library, Code 0142<br>Naval Postgraduate School<br>Monterey, CA 93943 | 2 |
| 3. | Department Chairman, Code 67<br>Department of Aeronautics<br>Naval Postgraduate School<br>Monterey, CA 93943 | 1 |
| 4. | Prof. Donald M. Layton<br>Code 67Ln<br>Naval Postgraduate School<br>Monterey, CA 93943 | 1 |
| 5. | Naval Air Systems Command<br>Attn: Mr Gibble, AIR-09E<br>Washington, DC 20360 | 1 |
| 6. | Naval Surface Weapons Center<br>Attn: Mr Sanchez, H-10<br>Dahlgren, VA 22448 | 1 |
| 7. | Naval Safety Center<br>Attn: Mr Kinney, System Safety<br>Norfolk, VA 23511 | 1 |
| 8. | U. S. Army Safety Center<br>Attn: CPT Mainwaring<br>Fort Rucker, AL 36360 | 1 |
| 9. | Lcdr Boyce W. Duke<br>4325 Calle de Vida<br>San Diego, CA 92124 | 2 |

211215

Thesis
D7877 Duke
c.1 A Program Manager's handbook for system safety and Military Standard 882B.